Toelichting bij 'Verklaring op eer COT'

Situering

Recent is er door de administraties en kabinetten van de federale en regionale overheden de modaliteiten vastgelegd rond de werking en vereisten van een zogenaamde 'Circle-of-Trust'.

Dit document is de toelichting bij deze modaliteiten.

Wat is een 'Circle of Trust' ?

Een 'Circle of Trust' is een concept dat zijn basis heeft in de cryptografie en in essentie betekent het dat binnen een bepaalde context (in dit geval : het eGezondheid ecosysteem) partijen (in dit geval : applicaties en systemen) elkaar vertrouwen dat elke partij de juiste maatregelen neemt op het vlak van toegang tot gegevens, registratie en gebruik van gegevens. Deze maatregelen gaan bv. over een sluitend gebruikersbeheer, een uitgewerkt toegangsbeheer waardoor de toegang tot systemen en data enkel gegeven wordt aan de rechtmatige gebruikers, of over logging en historiek van de toegangen tot de verschillende systemen.

Eenvoudig gesteld : binnen een bepaalde context vertrouwen verschillende systemen elkaar op het vlak van vertrouwelijkheid en gebruikersbeheer.
Een toepassing rekent erop dat een ander systeem alle nodige controles doet en dat een extra controle door de specifieke toepassing niet meer nodig is.

Waarom een 'Circle of Trust' ?

Het ecosysteem eGezondheid is een uitgebreid systeem van toepassingen en medisch-gerelateerde gegevens die voor een groot aantal gebruikers toegankelijk zijn.
Net omdat er zoveel verschillende systemen zijn én de behandelde data meestal gevoelige, medische informatie of privacy-gerelateerde gegevens bevat, is het voor een toepassing of applicatie meestal noodzakelijk om zich te verzekeren dat enkel bevoegde gebruikers toegang krijgen. Concreet betekent dit de een toepassing zelf een complex toegangsbeheer inbouwt (bv. met 2-step toegangscontrole, of met een specifiek hardware-toestel of met paswoord met een verplichte complexiteit).
Voor een gebruiker die verschillende systemen gebruikt én voor elk systeem een specifieke toegangscontrole moet doorlopen, kan dit leiden tot een onontwarbaar kluwen met veel tijdverlies tot gevolg. Uiteindelijk kan dit zelfs leiden tot een verminderde kwaliteit van de toegangscontrole als de gebruiker bv. zijn toegangscodes ergens noteert of overal dezelfde toegangscode gebruikt.

Het gebruik van het principe 'Circle of Trust' wil hieraan verhelpen. Het werkt als volgt :

- Een organisatie (bv. een zorginstelling) bevestigt expliciet, via een formele declaratie, dat de medewerkers (en andere gebruikers) toegang kunnen krijgen tot de applicatie(s) van de organisatie via een robuust toegangsbeheer, incl. logging, historiek en uitzonderingsbeheer ('Break the Glass'-procedures).

- Deze formele declaratie wordt geregistreerd op een plaats die toegankelijk is voor andere systemen en applicaties.
- Als een gebruiker van de organisatie, via een applicatie van die organisatie, toegang wil tot een ander systeem, zal het 'bestemmelings'-systeem op de gekende plaats opvragen of de organisatie de declaratie 'COT' heeft aangeduid.
- Als dit zo is, kan het 'bestemmelings'-systeem de gebruiker toegang geven zonder zelf de toegang te verifiëren.

- Dit betekent zowel voor de gebruiker een groot voordeel ('Single-Sign-on') als voor het 'bestemmelings'-systeem (geen complexe toegangscontrole te ontwikkelen).

Sommige systemen kunnen zelfs bepalen dat enkel gebruikers van organisaties die de COT-declaratie hebben aangegeven, toegang kunnen krijgen.

Wat is de 'Verklaring op eer COT' ?

De 'Verklaring op eer COT' is de manier waarop een organisatie kan aangeven dat ze alle regels van GDPR (o.a. een ernstig toegangsbeheer) toepast én dat de regels die bijkomend vastgelegd zijn voor het ecosysteem eGezondheid (o.a. via het eHealth Beheerscomité) volledig gevolgd worden.

De bijkomende regels voor het ecosysteem eGezondheid zijn o.a. gebruik van Informed Consent voor gegevensdeling, regels voor therapeutische relatie en uitsluitingen, toegangsmatrix, e.d.

De 'Verklaring op eer COT' wordt door de wettelijke vertegenwoordiger van de organisatie ondertekent. Het is de verantwoordelijkheid van de organisatie om dit document hetzij opnieuw ter ondertekenen, hetzij te herroepen als de omstandigheden veranderen, bv. bij overnames of fusies, bij wijziging van de gebruikte toepassingen, e.d.